The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation and Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein together with the Statement of inventorship and of right to grant of a Patent (Form 7/77), which was subsequently filed.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 13 August 2003

The Patent Office

7/77

Patents Act 1977
Rule 15

Statement of inventorship and of right to grant of a patent

The Patent Office
Concept House
Cardiff Road
Newport
South Wales NP10 8QQ

1.	Your reference	GB920020091GB1
2.	Patent application number *(if you know it)*	0314905.1
3.	Full name of the or of each applicant	INTERNATIONAL BUSINESS MACHINES CORPORATION
4.	Title of invention	**A SYSTEM FOR CONTROLLING ACCESS TO STORED DATA**
5.	State how the applicant(s) derived the right from the inventor(s) to be granted a patent	By employment and agreement
6.	How many, if any, additional Patents Forms 7/77 are attached to this form?	
7.		I/We believe that the person(s) named over the page (and on any extra copies of this form) is/are the inventor(s) of the invention which the above patent application relates to. R D Moss Signature 24 June 2003 Date R D MOSS
8.	Name and daytime telephone number of person to contact in the United Kingdom	A Sekar Tel: 01962 818169

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

LAMBERT, Howard Shelton
UK resident
c/o IBM United Kingdom Limited
Intellectual Property Law
Hursley Park
Winchester
Hampshire SO21 2JN
England

Patents ADP number *(if known)*

SPENCER, Gillian Laura
UK resident
c/o IBM United Kingdom Limited
Intellectual Property Law
Hursley Park
Winchester
Hampshire SO21 2JN
England

Patents ADP number *(if known)*

If there are more than three inventors, please write their names and addresses on the back of another Patents Form 7/77 and attach it to this form

WRIGHT, Steven
UK resident
c/o IBM United Kingdom Limited
Intellectual Property Law
Hursley Park
Winchester
Hampshire SO21 2JN
England

Patents ADP number *(if known)*

REMINDER

Have you signed the form?

The Patent Office

1/77

Patents Act 1977
Rule 16

26JUN03 E818084-2 D00611
P01/7700 0.00-0314905.1

Request for grant of a patent

The Patent Office
Concept House
Cardiff Road
Newport
South Wales NP10 8QQ

1.	Your reference	GB920020091GB1
2.	Patent application number *(The Patent Office will fill in this part)*	0314905.1
3.	Full name, address and postcode of the or of each applicant *(underline all surnames)*	INTERNATIONAL BUSINESS MACHINES CORPORATION Armonk New York 10504 United States of America
	Patents ADP number *(if you know it)*	00519637001
	If the applicant is a corporate body, give the country/state of its incorporation	State of New York United States of America
4.	Title of the invention	**A SYSTEM FOR CONTROLLING ACCESS TO STORED DATA**
5.	Name of your agent *(if you have one)*	R D Moss
	"Address for Service" in the United Kingdom to which all correspondance should be sent *(including the postcode)*	IBM United Kingdom Limited Intellectual Property Department Hursley Park Winchester Hampshire S021 2JN
	Patents ADP number *(if you know it)*	06547966003

6.	If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number	Country	Priority App No *(if you know it)*	Date of filing *(day/month/year)*
7.	If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date or the earlier application	No of earlier application		Date of filing *(day/month/year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.)

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	7
Claim(s)	2
Abstract	1
Drawing(s)	5 + 5

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	4
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application

R. D. Moss

Signature

24 June 2003
Date

R D MOSS

12. Name and daytime telephone number of person to contact in the United Kingdom

A Sekar
01962 818169

A SYSTEM FOR CONTROLLING ACCESS TO STORED DATA

FIELD OF THE INVENTION

This invention relates generally to the control of access to stored data.

BACKGROUND OF THE INVENTION

An example of such a service is the dispensing of cash by an automatic teller machine (ATM). Access to facilities provided by the ATM are typically controlled by requiring a user to present a personalised plastic card carrying data on a magnetic stripe to a card reader associated with the ATM. The user is required to key in a personal identification number (PIN) which is used by the system to access data in the card which together with data held in the system relating to the user enables the system to determine whether the requested transaction should be authorised.

The principle has been considerably extended to many types of transactions including the purchase of goods in retail outlets, access to processes on computer networks and the provision of stockbroking services. As the sophistication of the services has increased so has the need for increased flexibility and security in the control of access. For example, it is important that providers of services through retail tills/terminals or ATM's are assured that such services may only be accessed by authorised end-users with a valid access card, at a valid till and, where appropriate, under the control of an authorised sales assistant or other operator. Applications providing services may be held on the system in an encrypted form requiring a decryption key to access them, and the decryption key is then only provided to identified authorised users when they present a valid access card. It is also desirable to provide an audit trail for each transaction to facilitate the detection of fraud and the settlement of any dispute that may arise from the transaction.

An improved form of plastic card, called the Smart Card, has been developed which by incorporating within it active data processing and storage facilities provides enhanced security and flexibility. Data and application programs can be made inaccessible until an authorised person (as identified by personal information input by that person) presents their SmartCard. The present invention is suitable for use with SmartCards but is not limited thereto.

A problem arises when seeking to control access to application program modules where a number of different users are required to be allowed to access different sets of application modules. For example, in a retail environment, it may be desirable for all till operators to run certain applets associated with sales whereas only the store manager can access other applets associated with stock control or payroll. In another example, multiple users accessing data, applications or services on a shared device (e.g. a personal computer) require access to their applicable data, applications or services without compromising the privacy of the other users.

Preferably, a secure method of accessing user specific data or applications is required. The conventional approach to the problem of secure access in a shared environment is for a computer LOG ON procedure to include identification of the user from user input data (and optionally additional data held on a token such as a SmartCard). A table lookup process then scans a static list to determine the access authority of the user, and the user is given access to certain applications according to their determined authority level.

Such conventional systems relying on lookup tables of user authorities are vulnerable to breaches of security even if the applications themselves are held in a protected (e.g. encrypted) form if the list can be tampered with. An unauthorised person may seek to add themselves to the list or to change their authority level within the list.

GB Patent Application No. 2329497 discloses one solution to this problem. The security of stored data and applications is improved by an access control system and method in which user keys for accessing the stored data/services are representative of the user's level of authority, such that there is no need to maintain a separate lookup table of user authority levels. This removes a potential security exposure from the system. The user keys are hierarchical, including data for generating a plurality of different access keys for each of a plurality of different access levels. The access keys may be decryption keys for encrypted data or application programs.

DISCLOSURE OF THE INVENTION

According to a first aspect, the present invention provides a data processing system for controlling access of at least one user to stored data comprising: means, responsive to a request from the user to access a set of the stored data, for authenticating the user; means, responsive to

successful authentication, for decrypting an encrypted data structure associated with the user, wherein the data structure comprises data associated with the set; and means, responsive to successful decryption, for accessing the set.

Preferably, the data associated with the set comprises data associated with the location of the set and data associated with decryption of the set, if the set has been encrypted. In one embodiment, the set comprises all of the stored data. In another embodiment, the set comprises a portion of the stored data.

Preferably, the user request is initiated by presentation of a token by the user. In one embodiment, the token is a SmartCard. In a preferred embodiment, the token comprises means associated with the identity of the user. In one embodiment, the means associated with the identity of the user is a key. In another embodiment, the means associated with the identity of the user is a digital certificate. Preferably, the means associated with the identity of the user is derived from one or more biometric characteristics associated with the user, for example, a facial characteristic or a fingerprint.

In a preferred embodiment, the token comprises the means for decrypting the encrypted data structure. In one embodiment, the means for decrypting is the same as the means associated with the identity of the user (e.g. a key).

Preferably, the stored data is capable of access by more than one user (i.e. a shared system). In this case, the system further comprises means for accessing a data structure comprising data associated with each user of the more than one user. Preferably, the data structure is unencrypted and comprises data associated with the users that have access to the system (e.g. user name) and the location of each of the users' associated data structure.

Preferably, the data includes applications or services or both. In one embodiment, the data is stored on a remote system. In a preferred embodiment, the data structures are stored on the system. In an alternative embodiment, the encrypted data structure associated with the user is stored on the token. Advantageously, the data structures are easy to maintain e.g. to handle a change in the data that the user has access to; to handle addition/removal of users that have access to the system, etc.

According to a second aspect, the present invention provides a method for controlling access of at least one user to stored data via a data

processing system comprising the steps of: in response to a request from the user to access a set of the stored data, authenticating the user; in response to successful authentication, decrypting an encrypted data structure associated with the user, wherein the data structure comprises data associated with the set; and in response to successful decryption, accessing the set.

According to a third aspect, the present invention provides a computer program comprising program code means adapted to perform the steps of the method described above, when said program is run on a computer.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of example only, with reference to preferred embodiments thereof, as illustrated in the following drawings:

FIG. 1 shows an environment in which the present invention may be implemented;

FIG. 2 shows a more detailed overview of the environment of FIG.1, wherein a user accesses a device;

FIG. 3 shows a more detailed overview of the environment of FIG.1, wherein a user accesses a shared device;

FIG. 4 is a flow chart showing the operational steps involved when a user accesses a device as shown in FIG. 2; and

FIG. 5 is a flow chart showing the operational steps involved when a user accesses a shared device as shown in FIG. 3.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 shows a pictorial representation of an environment (100) in which a preferred embodiment of the present invention may be implemented. There is shown multiple users (105), each having access to a shared device (110) (e.g. a personal computer, a personal digital assistant (PDA) etc.).

Referring to FIG. 2 and FIG. 4, there is shown an overview of an environment wherein a user has access to a device (110), the device comprising stored data. Preferably, a user presents (step 400) a token

(200) (e.g. a SmartCard) to the device (110). Preferably, a user identity authentication means is stored on the SmartCard (200), for example a key. In one embodiment, a user enters some personal data (e.g. a Personal Identification Number (PIN)) after the SmartCard (200) is presented to the shared device (110) and a hashing algorithm is applied to the PIN in order to dynamically generate a key on the SmartCard (200) itself. However in a more advanced system the key may be generated from biometric data read by a reader adapted to recognise particular facial or other characteristics of the user such as fingerprint or hand geometry. In an alternative embodiment, an authentication key is pre-generated and stored on the SmartCard (200). In yet another embodiment, the user identity authentication means is a digital certificate comprising a key and a user id.

Upon presentation (step 400) of the SmartCard (200) to the device (110), in the example described herein, a key is generated in order to identify the user. The device (110) comprises means for authenticating (step 405) the key and in this way, the identity of the user is authenticated.

If authentication succeeds (positive result to step 410), preferably, decryption means on the SmartCard (200) (e.g. the same key used to authenticate the user, or another key) is used to decrypt (step 420) an encrypted "user specific table" (205) stored on the shared device (110). Alternatively, the decryption means can be stored on the device (110). Successful decryption allows the user (105) to access the table, whereby the table comprises data associated with a set of the stored data that the user has access to. In one embodiment, the set comprises all of the stored data. In another embodiment, the set comprises a sub-set of the stored data.

Preferably, the table identifies the name(s) of the stored data (e.g. Program 1, Program 2, Program 3, Program n); the location of the stored data in storage (210, 220) on the device (110) (i.e. "Location", a URL (Universal Resource Locator) etc.); and a decrypt key needed to decrypt the stored data if the data has been stored in an encrypted form. If the data has not been stored in an encrypted form, a decrypt key is not required. Once the user has accessed his/her user specific table, he/she gains access (step 425) to the set of stored data as required e.g. via hyperlinks, pointers etc.

The table (205) is encrypted so that only the authenticated user can view the table that is applicable to him/her (via an appropriate decrypt process). Therefore, the function of the user specific table (205) is to

identify the set of stored data that is available to the authenticated user.

If authentication does not succeed (negative result to step 410), appropriate action is taken (step 415), for example, a "warning" message or a "retry" message is displayed to the user. It should be understood that in the case of authentication failure, preferably, the user will not be able to access any functionality on the device at all. For example, the user will not be able to view the data that is installed. Alternatively, the user's access to functionality on the device (110) is restricted.

Referring to FIG. 3 and FIG. 5, there is shown an overview of an environment wherein a user accesses a device (110) shared amongst multiple users. The device comprises stored data. Preferably, each user has an associated token, in this example, a SmartCard (200), whereby a user identity authentication means is stored on their SmartCard (200). As described above, the user identity authentication means is a key, a digital certificate etc. In this example, the user's user identity authentication means is a key. Preferably, for each user, a corresponding user specific table exists (i.e. tables 205 and 305 in FIG. 3) on the device (110), each of the tables being individually encrypted.

Firstly, the user (A) presents (step 500) their SmartCard (200) to the device (110) in order to request access to a set of the stored data. Next, the user identity authentication means (in this example, a pre-generated key) is authenticated by authentication means on the device (110). This allows authentication (step 505) of the user. If authentication succeeds (positive result to step 510), the user is pointed (step 520) to an unencrypted table (300), which stores details of all the users that have access to the device (110) ("Personality") and the location of each of the users' user specific table ("Location").

Next, decryption means on the SmartCard (200) (e.g. a key) is used to attempt to decrypt (step 525) each of the user specific tables (i.e. tables 205 and 305) in turn until a successful decryption occurs. It should be understood that the location of the user specific tables has been provided by table 300. As shown in FIG. 3, the authenticated user has successfully decrypted table 205 and therefore gains (step 530) access to his/her "user specific table" (205), which comprises data associated with the set of the stored data that the user has access to. By encrypting user specific tables so that only the corresponding user can decrypt the table, each user has access only to the table that is applicable to him/her. This enables "personalities" to be assigned to the shared device (100) so that when an

authenticated user logs on to the device, only the set of the stored data, that is applicable to that user, is made available.

If authentication does not succeed (negative result to step 510), appropriate action is taken (step 515), for example, a "warning" message or a "retry" message is displayed to the user. It should be understood that in the case of authentication failure, preferably, the user will not be able to access any functionality on the device at all. Alternatively, the user's access to functionality on the device (110) is restricted.

While the present invention has been described above in relation to access to a shared device, it will be appreciated that it is applicable in any situation where access is sought to processes or other potentially sensitive material in the course of a token initiated transaction. For example it may readily be applied to environments such as the Internet in which access is sought to software and may only be granted if the requestor is appropriately authorised.

The present invention can be advantageously applied to thin clients, which have little or no application logic (e.g. mobile phones, PDAs etc.) since thin clients such as mobile phones already have processing capability. Advantageously, little modification of existing hardware is required in order to enable the thin clients to make use of the access control mechanism of the present invention.

CLAIMS

1. A data processing system for controlling access of at least one user to stored data comprising:

means, responsive to a request from the user to access a set of the stored data, for authenticating the user;

means, responsive to successful authentication, for decrypting an encrypted data structure associated with the user, wherein the data structure comprises data associated with the set; and

means, responsive to successful decryption, for accessing the set.

2. A data processing system as claimed in claim 1, wherein the data associated with the set comprises data associated with the location of the set.

3. A data processing system as claimed in claim 1, wherein the set is encrypted and the data associated with the set comprises data associated with decryption of the set.

4. A data processing system as claimed in any preceding claim, wherein the set comprises all of the stored data.

5. A data processing system as claimed in any of claims 1 to 3, wherein the set comprises a portion of the stored data.

6. A data processing system as claimed in any preceding claim, wherein the user request is initiated by presentation of a token by the user.

7. A data processing system as claimed in claim 6, wherein the token comprises means associated with the identity of the user.

8. A data processing system as claimed in claim 7, wherein the means associated with the identity of the user is derived from one or more biometric characteristics associated with the user.

9. A data processing system as claimed in claim 6, wherein the token comprises the means for decrypting.

10. A data processing system as claimed in any preceding claim, wherein the stored data is capable of access by more than one user, the system

further comprises means for accessing a data structure comprising data associated with each user of the more than one users.

11. A method for controlling access of at least one user to stored data via a data processing system comprising the steps of:

in response to a request from the user to access a set of the stored data, authenticating the user;

in response to successful authentication, decrypting an encrypted data structure associated with the user, wherein the data structure comprises data associated with the set; and

in response to successful decryption, accessing the set.

12. A computer program comprising program code means adapted to perform the steps of claim 11, when said program is run on a computer.

ABSTRACT

A SYSTEM FOR CONTROLLING ACCESS TO STORED DATA

A data processing system for controlling access of at least one user to stored data is provided. The system comprises means, responsive to a request from the user to access a set of the stored data, for authenticating the user. The system also comprises means, responsive to successful authentication, for decrypting an encrypted data structure associated with the user. The data structure comprises data associated with the set (e.g. location of the set). The system also comprises means, responsive to successful decryption, for accessing the set.

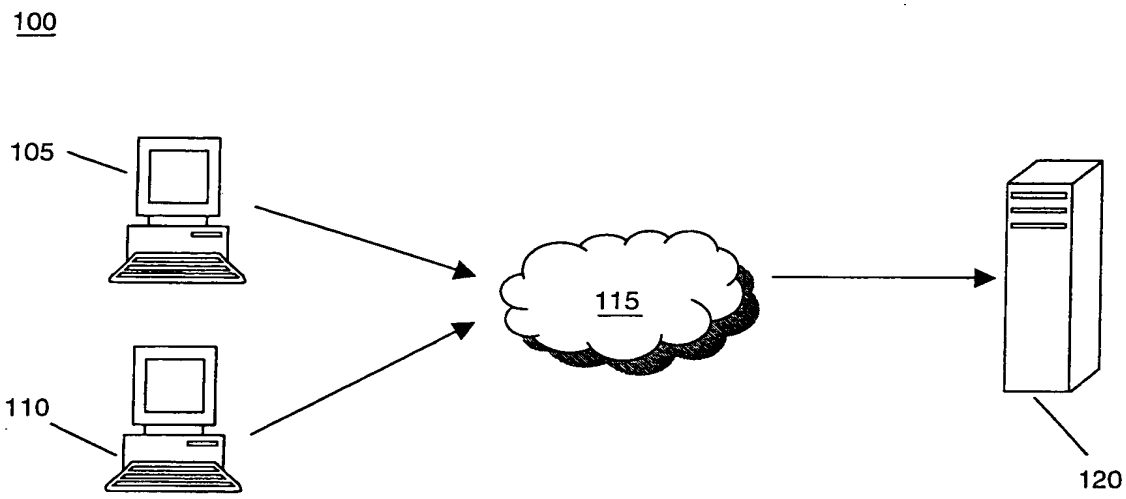

FIG. 1

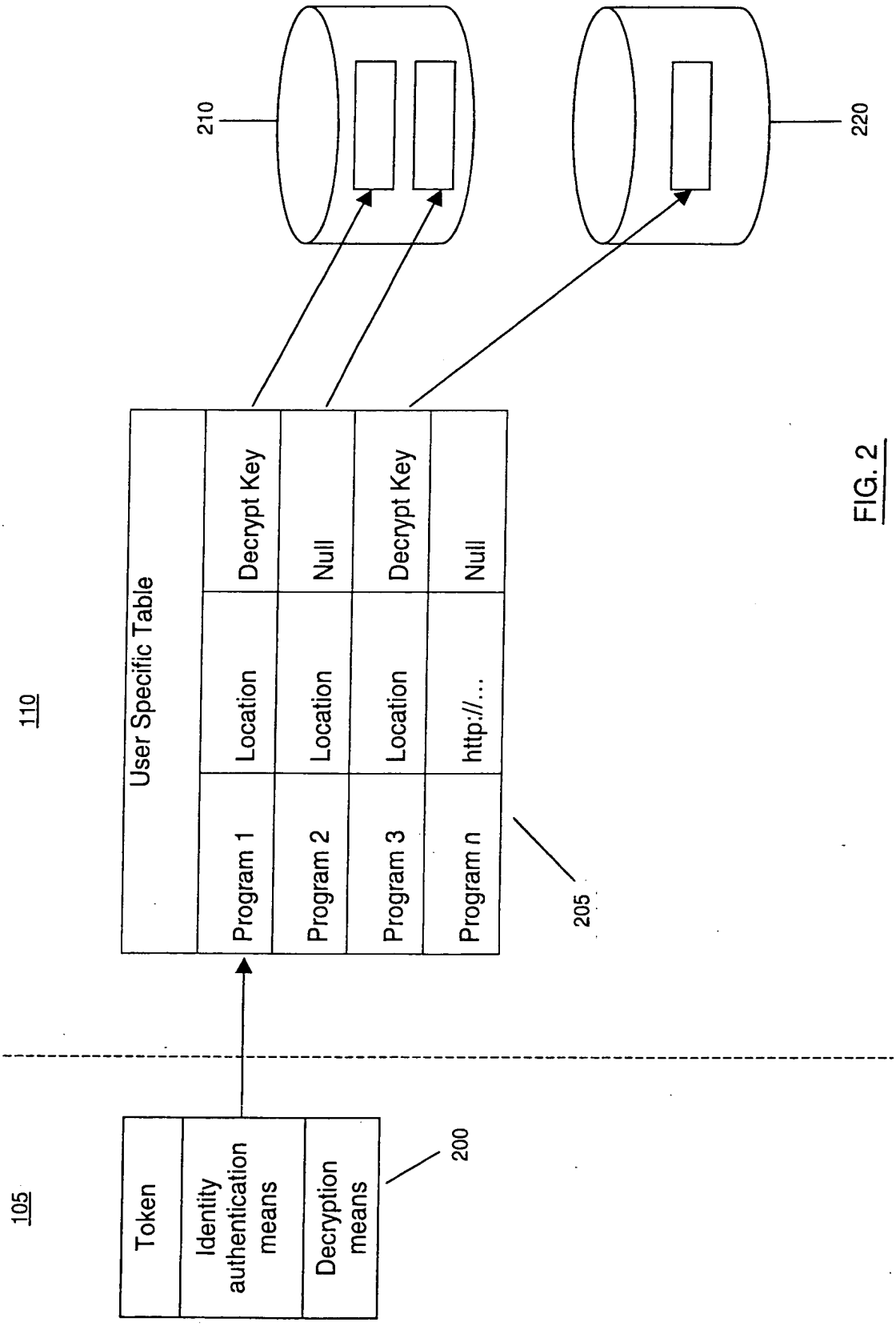
105
Token
Identity authentication means
Decryption means
200
110
User Specific Table
Program 1
Location
Decrypt Key
Program 2
Location
Null
Program 3
Location
Decrypt Key
Program n
http://...
Null
205
210
220

FIG. 2

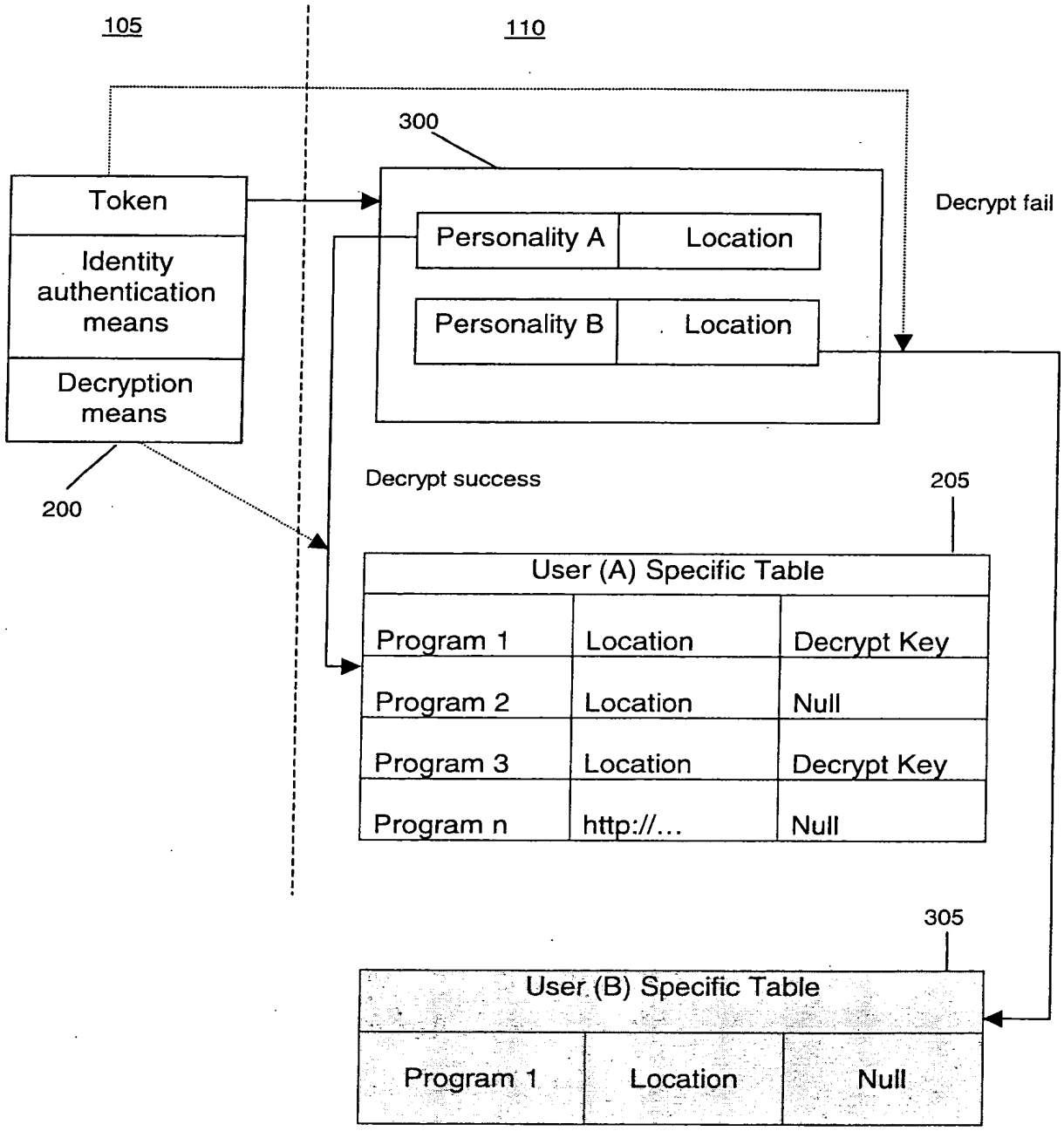
105
110
300
Token
Identity authentication means
Decryption means
200
Personality A
Location
Personality B
Location
Decrypt fail
Decrypt success
205
User (A) Specific Table
Program 1
Location
Decrypt Key
Program 2
Location
Null
Program 3
Location
Decrypt Key
Program n
http://...
Null
305
User (B) Specific Table
Program 1
Location
Null

FIG. 3

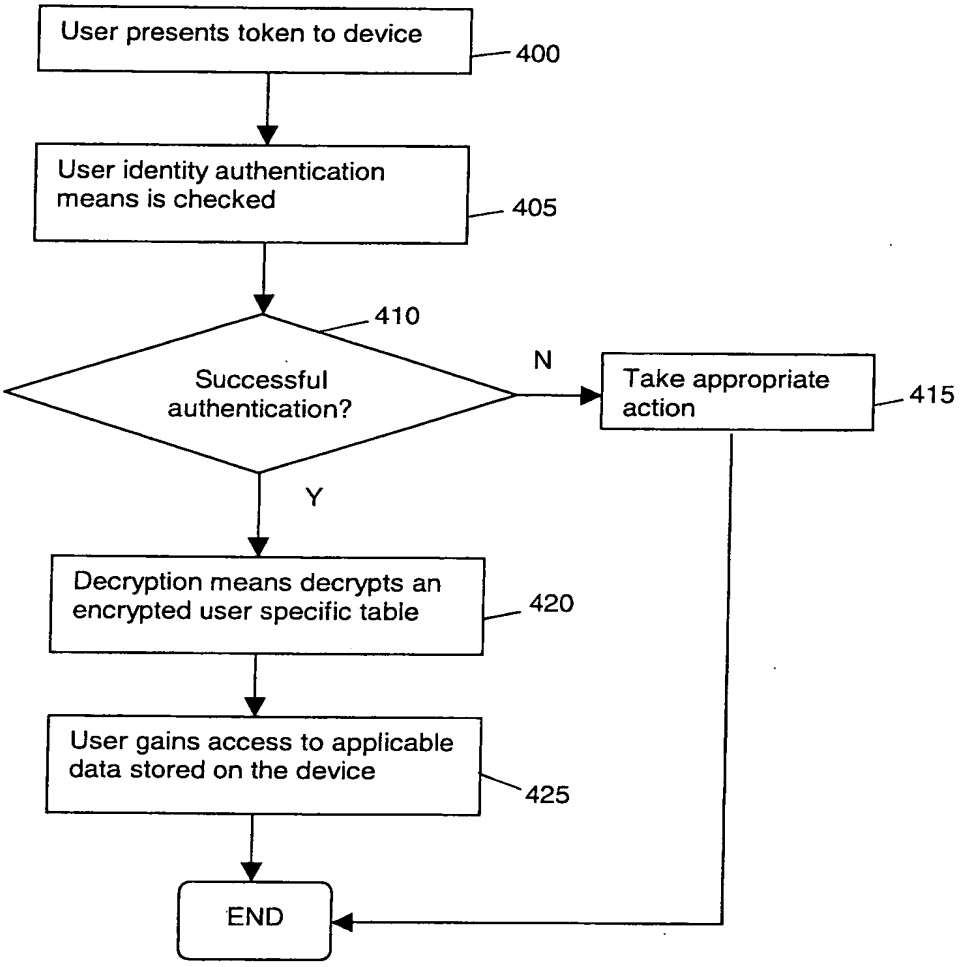
User presents token to device
400
User identity authentication means is checked
405
410
Successful authentication?
N
Take appropriate action
415
Y
Decryption means decrypts an encrypted user specific table
420
User gains access to applicable data stored on the device
425
END

FIG. 4

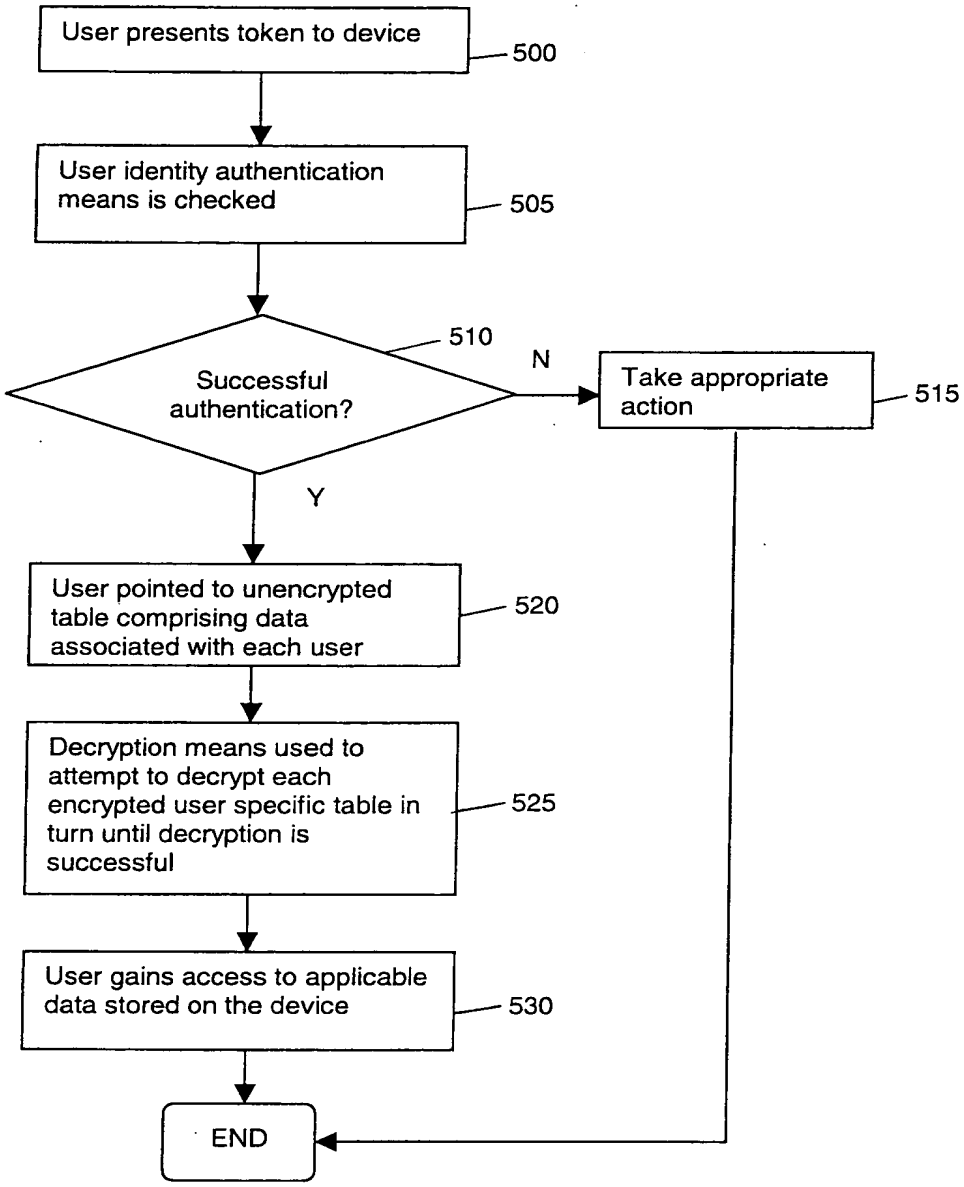
User presents token to device
500
User identity authentication means is checked
505
Successful authentication?
510
N
Take appropriate action
515
Y
User pointed to unencrypted table comprising data associated with each user
520
Decryption means used to attempt to decrypt each encrypted user specific table in turn until decryption is successful
525
User gains access to applicable data stored on the device
530
END

FIG. 5